claims are not being pursued herein since they will appear in an issued US patent in due
course. This divisional application is being directed to a specific feature disclosed in the
parent application where a mediator, for example, can be employed to protect against the
possibility that the owner refuses to send the consumer the necessary key to decode the
document thereby allowing the mediator to step in and to provide a key to aid in decoding the
document.

Claim 2 which was allowed in the parent application is amended herein to read somewhat
differently (see the discussion below). The claims which depend therefrom have been
amended to remove multiple dependencies in order to reduce the official fees which would
others be due.

Claims 7 and 10 - 11 have been amended to add limitations thereto to reflect the possible
presence of the second and fourth portions of the key. These claims, without these
limitations, as presently being prosecuted in the parent application

The Examiner also objected to the specification of the parent application because of various
minor informalities therein. As the Examiner will note, by reference to the amendments made
above, the formalities mentioned by the Examiner during the prosecution of the parent
application have been addressed.

The Examiner will note that the Applicants have amended claim 2, even though that claim was
allowed in the parent application. A marked-up copy of claim 2 showing the amendments
being made thereto can be found in the Appendix to this Response. The Examiner will note, in
comparing this claim with the version of claim 2 allowed by the examiner in the parent
application, that the language about the third portion of the key and the fourth portion of the
key being combined has been moved from step (c) to a step (d2). In the invention as
disclosed, that step would be utilized when the mediator gets involved, because the owner
failed to provide the second portion of the key in response to receiving the payment. Thus,
after the consumer provides the owner with the payment, either the owner provides a source
with a missing second portion of the key, so that the first and second portions can be

combined to generate a complete key or, if the owner does not provide the source with the second key portion, the third key portion can be combined with the fourth key portion to generate a complete key. As such, the limitation heretofore in step (c) in claim 2 as originally allowed in the parent application has been moved to step (d2).

The abstract has been shortened and formed now as a single paragraph.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to Deposit Account No. 12-0415 and, in particular, if this Response is not timely filed, then the Commissioner is authorized to treat this Response as including a petition to extend the time period pursuant to 37 CFR § 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to Deposit Account No. 12-0415.

I hereby certify that this correspondence is being deposited with the United States Postal Service as *express* mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C., 20231 on

_____January 18, 2002_____
(Date of Deposit)

_____RICHARD P. BERG_____
(Name of Applicant, Assignee
or Registered Representative)

(Signature)

_____January 18, 2002_____
(Date)

Respectfully submitted,

Richard P. Berg
Attorney for Applicant
Reg. No.: 28,145
LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, California 90036
(323) 934-2300

RPB:pm

Appendix:

At page 1, lines 16 - 22 the following amendment is being made:

--(a)   Matthew K. Franklin and Michael K. Reiter, *Fair Exchange with a Semi-Trusted Third Party*, Proceedings of the 4th ACM Conference on Computer and Communications Security, 1997; this document describes a fair exchange protocol with a semi-trusted third party with trust assumptions similar to those used in the present invention. The third party in this [inthis] case, however, is online even if the parties follow the protocol faithfully;--

At page 1, lines 27 and continuing through page 2, line 3 the following amendment is being made:

--(c)   N. Asokan, M. Schunter and M. Waidner, *Optimistic Protocols for Fair Exchange*, Proceedings of the 4th ACM Conference on Computer and Communications Security, 1997; this document describes a practical optimistic protocol for [fari] fair exchange. However, this protocol increases the trust requirements on the third party in the event of a dispute resolution being required. In particular, the third party inspects the contents of a message containing the item being exchanged while resolving disputes. In addition, the described protocol family has a synchronous time model which may not be suitable for certain applications.--

At page 2, lines 5 - 11 the following amendments are being made:

--In accordance with a first aspect of the present invention there is provided a cryptographic method of enabling a consumer to obtain a document from an owner upon a payment [as defined in Claim 1.

In accordance with a second aspect of the present invention there is provided a cryptographic method of enabling a consumer to obtain a document from an owner upon a payment as defined by Claim 2].--

At page 2, line 12 of the application the following amendment is being made:

--The first and third portions of [the] a key are preferably different.--

At page 2, lines 27 - 31 the following amendments are being made:

--In accordance with a third aspect of the present invention there is provided a document source for use in one of the above-described methods [as defined by Claim 7].

In accordance with a fourth aspect of the present invention, there is provided a document source [as defined by Claim 8].--

At page 3, lines 10 - 21 the following amendments are being made:

--In accordance with a fifth aspect of the present invention, there is provided a fair exchange method of enabling a consumer to obtain a document from an owner upon a payment [as defined by Claim 14].

In accordance with a sixth aspect of the present invention there is provided a cryptographic method of enabling a first party to obtain an item of value from a second party upon receipt by said second party of a second item of value [as defined by Claim 15].

In accordance with a seventh aspect of the present invention there is provided a fair exchange method of enabling a contract between a buyer and a seller of a commodity [as defined in Claim 16].--

At page page 4, lines 18 - 22 the following amendment is being made:

--As can be seen from the above, there is a distinction between the two roles of the consumer and the printer. This is important, because of the underlying trust assumption, namely that the printer can be entrusted by the owner to respect the conditions of a copyright agreement, whereas it may not be reasonable to assume that the consumer would do the same.--

The following amendments are being made to the claims:

2. (Amended) A cryptographic method of enabling a consumer to obtain a document from an owner upon making a payment, the method comprising [the use] a step of using a protocol involving the consumer, the owner, [and] a document source and a mediator, wherein the source requires knowledge of a key in which said document is encrypted in order to provide the said document, said key comprising a first portion, a second portion, a third portion, and a fourth portion, the protocol comprising the following sequential steps:

(a) the consumer requests a specified document;

(b) the owner provides the source with the first and third portions of the key and provides a mediator with the fourth portion of the key, which can combine with the third portion of the key to generate [the] a complete key;

(c) the consumer provides the owner with the payment;
and either:

(d1) the owner provides the source with the second portion of the key and said first portion of the key is combined [, which can combine] with said second portion of the key to

generate [the] a complete key; or

       (d2) the owner does not provide the source with the second key portion, and the third key portion is combined with the fourth key portion to generate a complete key.

4.   (Amended) A cryptographic method as claimed in Claim 2 [or Claim 3], and arranged for enabling a said consumer to receive a plurality of such documents, wherein said first and second portions are different for each document.

5.   (Amended) A cryptographic method as claimed in [any one of] Claim[s] 2 [to 4], wherein the mediator is involved in the protocol only in the event of a dispute between the owner and the consumer.

6.   (Amended) A cryptographic method as claimed in [any preceding claim] Claim 2, wherein the document source comprises a printer.

7.   (Amended) A printer [document source] for use in [a method as claimed by any preceding claim, the source comprising] enabling a consumer to print a document from an owner upon making a payment, the printer including:

       (a) a memory for storing a first key portion and a third key portion;

       (b) an element [means] for receiving a [said] second key portion or a fourth key portion; and

       (c) an element [means] for decrypting an encrypted document transmitted thereto in accordance with an encryption key defined by said first and said second key portions or said third and said fourth key portions.

10.   A [document source] printer as claimed in Claim [9] 7, arranged to print a number of copies of a said document in each of a plurality of formats.

11.   A [document source] printer as claimed in Claim 10, arranged to print only one copy of a said document in a first format and an unlimited number of copies of said document in a second format.

12.   A [document source] <u>printer</u> as claimed in Claim 10 [or Claim 11], wherein said formats comprise different resolutions.

13.   A [document source] <u>printer</u> as claimed in [any one of] Claim[s] 10 [to 12], wherein said formats comprise monochrome and [colour] <u>color</u> images.

The following amendments are being made to the abstract:

A document transfer system enabling a consumer to obtain a document from an owner upon payment uses a cryptographic protocol involving the consumer, the owner, a document source, such as a printer, and a mediator. [, the protocol comprising the following steps:

(a)   the consumer requests a document;

(b)   the owner provides the source with first and third portions of the key and provides the mediator with a fourth portion of the key, which can combine with said first portion to generate the complete key;

(c)   the consumer provides the owner with the payment; and

(d)   the owner provides the source with a second portion of the key, which can combine with said first portion to generate the complete key.

A printer 1 for use in the above system comprises a document memory 2 for storing a received encrypted document, a key memory 3 for storing a first cryptographic key portion, a processor 4 for receiving a second cryptographic key portion and combining it with the first key portion to form a complete cryptographic key which is supplied to a decrypting module 5. The encrypted document is supplied to the decrypting module 5 whereupon the document is decrypted and supplied to the consumer.]